

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 8 - 1 6 0 8 5 6

(43) 公開日 平成 8 年 (1996) 6 月 21 日

(51) Int. Cl.<sup>6</sup> 識別記号 庁内整理番号 F I 技術表示箇所  
G09C 1/00 7259-51  
H04L 9/00  
9/10  
9/12

H04L 9/00 2  
審査請求 未請求 請求項の数 19 O L (全 11 頁)

(21) 出願番号 特願平 6 - 2 9 9 9 4 0

(22) 出願日 平成 6 年 (1994) 12 月 2 日

(71) 出願人 0 0 0 0 0 4 2 2 6

日本電信電話株式会社

東京都新宿区西新宿三丁目 19 番 2 号

(72) 発明者 高嶋 洋一

東京都千代田区内幸町 1 丁目 1 番 6 号 日

本電信電話株式会社内

(72) 発明者 石井 晋司

東京都千代田区内幸町 1 丁目 1 番 6 号 日

本電信電話株式会社内

(72) 発明者 山中 喜義

東京都千代田区内幸町 1 丁目 1 番 6 号 日

本電信電話株式会社内

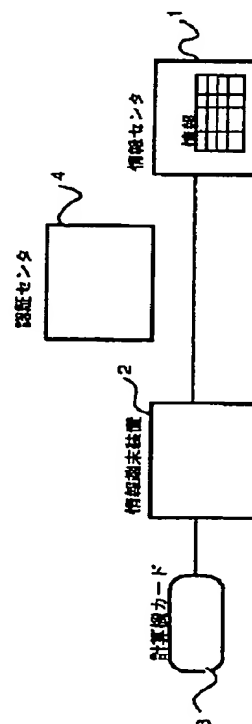
(74) 代理人 弁理士 吉田 精孝

(54) 【発明の名称】 デジタル情報保護システム及びその方法

(57) 【要約】

【目的】 情報が第 3 者に漏れることなく、正しい利用者であっても違法コピーが困難なデジタル情報保護システム及びその方法を提供する。

【構成】 情報端末装置 2 から利用者が選んだ利用情報の情報識別子を計算機カード 3 へ送って署名を受け、これを情報センタ 1 に送信し、情報センタ 1 では利用情報を暗号化するための鍵 W K を生成するとともに利用情報を該鍵 W K で暗号化して情報端末装置 2 に蓄積し、また、計算機カード 3 から利用情報が蓄積されたことを示す署名とともに配達証明のための乱数を情報センタ 1 に送り、情報センタ 1 で鍵 W K を前記乱数で変換して計算機カード 3 に配送し、計算機カード 3 から鍵 W K を情報端末装置 2 にセットした後、前記蓄積された利用情報を該セットされた鍵 W K で復号する。



## 【特許請求の範囲】

【請求項 1】 共通鍵暗号方式もしくは公開鍵暗号方式の公開鍵により暗号化されたデジタル情報を情報センタから通信回線、無線、パッケージメディア等を介して情報端末装置に蓄積し、利用する前に計算機カード内に秘密の復号鍵WKを情報センタから得て、利用する毎に計算機カード内の復号鍵WKで情報端末装置に暗号化されて蓄積された情報を復号しつつ情報端末装置にて利用することを特徴とするデジタル情報保護システム。

【請求項 2】 情報センタは、デジタル情報を蓄積する情報蓄積手段と、情報端末装置との通信を行う通信制御手段と、情報暗号鍵及び復号鍵を生成する鍵生成手段と、デジタル情報を暗号化する暗号化手段と、鍵を暗号通信するための公開鍵暗号化手段と、署名を行うための署名（公開鍵暗号復号）変換手段と、配達証明用の情報変換手段とを具備したことを特徴とする請求項 1 記載のデジタル情報保護システム。

【請求項 3】 情報端末装置は、情報センタとの通信を行う通信制御手段と、計算機カードとの通信を行う通信制御手段と、デジタル情報を蓄積する情報蓄積手段と、鍵を暗号通信するための公開鍵暗号化手段と、署名を行うための署名（公開鍵暗号復号）変換手段と、乱数を発生する乱数発生手段と、前記乱数と計算機カードから受信した乱数との値を照合する照合手段と、自装置の秘密鍵を格納する秘密鍵蓄積手段と、鍵情報及びデジタル情報を復号する復号手段と、前記乱数発生手段、照合手段、秘密鍵蓄積手段及び復号手段の機密を物理的に保護する機密保護手段とを具備したことを特徴とする請求項 1 記載のデジタル情報保護システム。

【請求項 4】 計算機カードは、情報端末装置との通信を行う通信制御手段と、鍵を暗号通信するための公開鍵暗号化手段と、署名を行うための署名（公開鍵暗号復号）変換手段と、配達証明用の情報変換手段とを具備したことを特徴とする請求項 1 記載のデジタル情報保護システム。

【請求項 5】 請求項 2 記載の情報センタと、請求項 3 記載の情報端末装置と、請求項 4 記載の計算機カードとを備えたことを特徴とする請求項 1 記載のデジタル情報保護システム。

【請求項 6】 計算機カードと情報端末装置が相互に認証し、

計算機カードが利用者を確認し、

利用者の要求情報に署名してさらに暗号化して情報センタにアクセスし、

暗号化された利用情報を情報端末装置に蓄積し、蓄積されたことを示す受領署名を情報センタへ返送し、

利用情報を復号するための鍵WKを利用の前に計算機カードに登録し、鍵WKが配送されていることを配達証明によって保証し、

計算機カードから鍵WKが情報端末装置にセットされた

後、情報端末装置に蓄積された暗号化情報を情報端末装置で復号しながら、その情報を利用することと、要求情報と暗号化情報の受領署名と配達証明情報を課金根拠として記録することを特徴とするデジタル情報保護方法。

【請求項 7】 計算機カードと情報端末装置が相互に認証する方法として、情報端末装置が生成した乱数を計算機カードに送り、計算機カードが署名暗号化したものを情報端末装置が受け取り、元の乱数と辻褄が合っているか否かをチェックすることを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 8】 計算機カードが情報端末装置を操作する利用者を認証する方法として、予め定めたパスワードを計算機カードに格納しておき、情報端末装置から入力された文字列が一致するかどうかをチェックし、入力誤りが所定の回数を越えた時はエラー処理し、該エラーが一定の回数続けて繰り返された場合は計算機カードを無効とするように制御することを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 9】 計算機カードが情報端末装置を操作する利用者を認証する方法として、予め定めたパスワードを計算機カードに暗号化して格納しておき、情報端末装置から入力された文字列が暗号化したものと一致するか否か（又は計算機カードに格納された暗号化されたパスワードを復号したものが情報端末装置から入力されたものと一致するか否か）をチェックすることを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 10】 計算機カードが情報端末装置を操作する利用者を認証する方法として、予め定めたパスワードを計算機カードに暗号化して又はそのまま格納しておき、情報端末装置から入力された文字列を、情報端末装置と計算機カードとの間で暗号通信し、入力された文字列が暗号化したもの又はそのままのものと一致するか否かをチェックし、一致しているか否かによって生成した乱数のパリティを調節し、その乱数を暗号通信することを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 11】 計算機カードが情報端末装置を操作する利用者を認証する方法として、予め定めたパスワードを計算機カードに暗号化して又はそのまま格納しておき、情報端末装置から入力された文字列に情報端末装置で生成した乱数を加えて（あるいは排他的論理和をとって）、情報端末装置と計算機カードとの間で暗号通信し、計算機カードで送られてきた文字列から予め登録してあるパスワードを引き（あるいは排他的論理和をとって）、得られた値を情報端末装置に返送し、情報端末装置で生成した乱数と返送された値とが一致するか否かでチェックすることを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 12】 利用者が選んだ情報の情報識別子と情報センタの公開鍵とその証明書とを計算機カードへ送信

し、計算機カードが情報識別子に署名暗号化し、情報端末装置でそれに計算機カードの公開鍵とその証明書を付け加えて情報センタに送信することにより、情報センタへの不正アクセスを防止することを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 1 3】 利用者が選んだ情報の情報識別子と情報センタの公開鍵とその証明書とを計算機カードへ送信し、計算機カードが情報識別子に署名したもの（RQ S）を暗号化し、情報端末装置でそれに計算機カードの公開鍵とその証明書を付け加えて情報センタに送信し、復号することにより RQ S を得て配達証明に利用することを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 1 4】 利用情報を暗号化するための鍵 WK を情報センタが生成し、該鍵 WK で利用情報を暗号化し、暗号化情報に対してデータ圧縮等の適当なアルゴリズム（ハッシュアルゴリズム）を施した後、署名したものととも情報端末装置へ送信し、暗号化情報は蓄積し、署名は計算機カードにて検証を行い、情報要求とともに暗号化情報が蓄積された情報端末装置の識別番号を計算機カード内へ登録することを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 1 5】 計算機カードが暗号化情報にハッシュアルゴリズムを施した後に署名し、情報センタへ送り、情報センタがその署名を検証することによって暗号化情報が情報端末装置に正しく蓄積され、計算機カードにその情報識別子が登録されていることを確認することを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 1 6】 情報センタと計算機カードとの間で鍵 WK が正しく配送されていることを保証する配達証明プロトコルを利用したことを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 1 7】 計算機カードで WK 要求メッセージ内の乱数と鍵 WK を結合し、情報端末装置の公開鍵で暗号化して情報端末装置に送信し、情報端末装置でそれを復号した後、乱数が一致するか否かをチェックし、鍵 WK をセットし、蓄積された暗号化情報を復号することを特徴とする請求項 6 記載のデジタル情報保護方法。

【請求項 1 8】 一の情報端末装置に計算機カードを接続して購入した暗号化情報を、他の情報端末装置に前記計算機カードを接続して利用する場合、自動的に暗号化情報を一の情報端末装置から取り寄せて他の情報端末装置に蓄積することを特徴とする請求項 6 又は 1 4 記載のデジタル情報保護方法。

【請求項 1 9】 一の情報端末装置に計算機カードを接続して購入した暗号化情報を、他の情報端末装置に前記計算機カードを接続して利用する場合、自動的に暗号化情報を一の情報端末装置から取り寄せて他の情報端末装置で復号しつつ利用することを特徴とする請求項 6 又は 1 4 記載のデジタル情報保護方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、音楽、映像、プログラム等のデジタル情報の不正な複製を防止し得るデジタル情報保護システム及びその方法に関するものである。

【0002】

【従来の技術】 近年、音声・動画・静止画等のデジタル情報圧縮技術（例えば、MPEG = Moving Picture Experts Group、JPEG = Joint Photographic Coding Experts Group 等）及び ISDN を代表とする高速デジタル通信技術の発達により、音楽・映像・絵画・書籍等の著作物をデジタル情報に変換し圧縮符号化して、情報センタ等から通信回線を介して各利用者端末へ配送することが可能となってきた。

【0003】 前述した映像等のデジタル情報に比べてデータ量の少ないコンピュータソフトウェアについては、既にパソコン通信等を利用して配送サービスを実施している例がある。また、最近、米国内においてサービスが開始された CD-ROM によるコンピュータソフトの販売方法では、暗号化された販売用ソフト及び暗号化されていないデモ用ソフトを格納した CD-ROM を低価格で販売・配布し、デモ用ソフトを試用した利用者が購入希望を電話等でサービスセンタに申込みと、該利用者に復号鍵を通知して暗号化された販売用ソフトの使用を可能とする形式をとっている。

【0004】

【発明が解決しようとする課題】 前述した従来のパソコン通信等によるソフトウェアの販売方法の場合、ソフトウェアの暗号化がなされておらず、フロッピーディスク等のパッケージによるソフトウェアの販売方法に比べて、違法コピーをより容易にさせる環境を提供してしまうという問題があった。

【0005】 また、前述した CD-ROM によるソフトウェアの販売方法の場合、電話等にて復号鍵をサービスセンタより受け取る際にセンタオペレーションを介するため、人手がかかり、かつ利用者のプライバシーを保つことができないという問題があった。また、人手を介するため、復号鍵の横流し等の不正により違法コピーが可能になるという問題があった。

【0006】 本発明の目的は、情報が第 3 者に漏れることなく、正しい利用者であっても違法コピーが困難なデジタル情報保護システム及びその方法を提供することにある。

【0007】

【課題を解決するための手段】 本発明では前記目的を達成するため、物理的に封印された装置を情報端末装置に入れ、復号するための鍵 WK を計算機カードに蓄積し、利用した証拠として、要求情報、鍵受領署名、配達証明情報を情報センタが記録することを特徴とする。

【 0 0 0 8 】

【作用】本発明によれば、情報を暗号化して配送しているため、情報が第三者に漏れる恐れがなく、また、復号鍵が計算機カードの中に閉じ込められており、正しい利用者ですら復号鍵を知ることが困難であることと、情報端末装置に物理的に封印してある装置で鍵WKの復号、情報の復号を行うため、違法コピーが困難であることと、配達証明情報により確実に課金を行えることから、情報提供者が安心して利用できるシステムとなる。

【 0 0 0 9 】

【実施例】図 1 は本発明のデジタル情報保護システムの一実施例を示すもので、図中、1 は情報センタ、2 は情報端末装置、3 は計算機カード、4 は認証センタである。

【 0 0 1 0 】情報センタ 1 は、情報提供者から供給された多数のデジタル情報を蓄積し、これをデータベースのように管理している。

【 0 0 1 1 】情報端末装置 2 は、デジタル情報を利用するための画像表示装置、音声出力装置等を具備し、各利用者の家庭等に配置されている。情報センタ 1 と情報端末装置 2 とは通信ネットワークを通じて相互通信可能のように接続されている。

【 0 0 1 2 】計算機カード 3 は、情報端末装置 2 に対して着脱自在に取り付けられ、どの情報を購入したかという取り引き内容を示すデータを内部に蓄積しておくことができる。この計算機カード 3 は利用者毎に所持することができ、各利用者はこの計算機カード 3 を情報端末装置 2 に接続することによって、購入済のデジタル情報（画像、音楽等）を情報センタ 1 から情報端末装置 2 に送らせて利用することができる。

【 0 0 1 3 】なお、認証センタ 4 は公開鍵暗号方式を利用する際の準備段階でのみ必要となる。

【 0 0 1 4 】（情報センタの構成）図 2 は情報センタの詳細な構成を示すもので、図中、11 は利用情報を入力する情報入力部、12 は利用情報を蓄積する情報蓄積部、13 は利用情報を暗号化する情報暗号化部、14 は利用情報を暗号化する時に用いる鍵WKを生成するWK生成部、15 は鍵WKを暗号化する公開変換部、16 は暗号化された鍵WKが情報センタのものであることを示すための署名変換部、17 は情報センタの公開鍵やその認証センタによる証明書や演算の途中結果等を記憶するためのメモリ、18 は情報センタ全体の制御とハッシュアルゴリズムや配達証明のための情報変換等を実行するCPU、19 は計算機カードの公開鍵等を検証する公開鍵検証部、20 はネットワークとのやりとりを行うネットワーク入出力部である。

【 0 0 1 5 】（情報端末装置の構成）図 3 は情報端末装置の詳細な構成を示すもので、図中、21 は計算機カード 3 とのやりとりを行うカード入出力部、22 は公開鍵暗号の復号を行う復号鍵抽出部、23 は利用情報の復号

を行う情報復号部、24 は復号された情報を出力する情報出力部、25 a は画像表示装置、25 b は音声出力装置、26 は復号鍵抽出部 22、情報復号部 23 及び情報出力部 24 の機密を物理的に保護する機密保護手段、27 は利用情報を暗号化されたまま蓄積する情報蓄積部、28 はネットワークとのやりとりを行うネットワーク入出力部、29 は情報端末装置の公開鍵や認証センタの証明書や演算の途中結果等を記憶するためのメモリ、30 は情報端末装置全体の制御と乱数生成やハッシュアルゴリズムを実行するCPUである。

10

【 0 0 1 6 】（計算機カードの構成）図 4 は計算機カードの詳細な構成を示すもので、図中、31 は認証センタの証明書で公開鍵が正当であることを検証する公開鍵検証装置、32 は暗号化や署名変換を施す公開鍵暗号装置、33 は情報端末装置 2 との通信を行う通信装置、34 は利用者認証のためのパスワード照合を行うパスワード照合装置、35 は購入情報の復号鍵を登録する復号鍵登録装置、36 は計算機カードの公開鍵やその証明書や演算途中結果を記憶するメモリ、37 は計算機カード全体の制御と乱数生成や配達証明のための情報変換等を行うCPU、38 は秘密鍵等の情報を保持するために必要な電圧監視装置、39 はバックアップ用の電池である。

20

【 0 0 1 7 】（情報利用プロトコル）

<事前準備> 情報Mを鍵Kで暗号化して暗号化情報Cを得る変換を  $C = EK(M)$  で表し、復号することを  $M = DK(C)$  で表す。特に公開鍵暗号方式を利用する時は暗号化を  $C = EK_i(M)$ 、復号を  $M = DK_i(C)$  で表す。後者は署名変換としても用いることがある。

30

【 0 0 1 8 】計算機カード 3 には予め識別子IDUと公開鍵KPUとその証明書XPUと認証センタ 4 の公開鍵KPCと秘密鍵KSUと秘密情報Sと公開情報n'とが書き込まれており、特に秘密鍵KSUと秘密情報Sは読み出せないように保護されたエリアに書き込まれる。なお、IDUとSとn'の間には  $IDU = S' \bmod n'$  の関係があり、n'は2つの大きな素数の積で数百ビット程度の大きさである。証明書XPUは認証センタ 4 で公開鍵KPUを認証してもらい、 $XPU = DK_{K_i}(XPU)$  として求められる。但し、KSCは認証センタ 4 の秘密鍵で、これは認証センタ 4 以外には秘密にされる。

40

【 0 0 1 9 】同様に、情報端末装置 2 には予め識別子IDSと公開鍵KPSとその証明書XPSと認証センタ 4 の公開鍵KPCと秘密鍵KSSとが書き込まれ、情報センタ 1 には予め識別子IDMと公開鍵KPMとその証明書XPMと認証センタ 4 の公開鍵KPCと秘密鍵KSMとが書き込まれる。また、計算機カード 3 には利用者を認証するための情報（例えばパスワード）が読み出されないように登録される。

【 0 0 2 0 】<計算機カード・情報端末相互認証> 図 5 は計算機カード・情報端末相互認証の工程を示すものである。

50

【0021】 計算機カード 3 が情報端末装置 2 に接続されると、情報端末装置 2 から、乱数 R と該情報端末装置 2 の公開鍵 KPS とその公開鍵の証明書 XPS と該情報端末装置 2 の識別子 IDS とが計算機カード 3 へ送られる。

【0022】 計算機カード 3 はその内部に保持している認証センタ 4 の公開鍵 KPC を利用して、情報端末装置 2 の公開鍵 KPS とその証明書 XPS との辻褄が合っているか否かを確認することにより、情報端末装置 2 の公開鍵 KPS が正当であるか否かを判断する。正当と判断された時は送られて来た乱数 R に署名暗号化変換を施し、 $T = E_{K_s}(DK_s, (R))$  (又は  $DK_s, (EK_s, (R))$ ) なる T と計算機カード 3 の公開鍵 KPU とその証明書 XPU と識別子 IDU とを情報端末装置 2 に送信する。

【0023】 情報端末装置 2 はその内部に保持している認証センタ 4 の公開鍵 KPC を利用して計算機カード 3 の公開鍵 KPU が正当であることを確認した後、送られてきた T と送った R との辻褄が合っているか否かを確認することにより、相手が正しい計算機カード IDU であるか否かを判断する。

【0024】 <利用者認証> 図 6 は利用者認証の工程を示すものである。

【0025】 利用者は、情報端末装置 2 に予め計算機カード 3 に登録してあるパスワードを入力する。情報端末装置 2 は入力されたパスワードを計算機カード 3 に送信し、正しいかどうかを判断してもらう。パスワードの入力が正しい場合には、正当な利用者であると判断し、メニュー情報を利用者に示す。

【0026】 この際、パスワードの入力誤りは予め定めた所定の回数、例えば 3 回まで許容し、3 回を越えた時はエラー処理、つまり正当な利用者でない可能性があるとして計算機カード 3 を排出し、さらに該エラーが予め定めた一定の回数、例えば 5 回続けて繰り返されたような場合は正当な利用者でないとして該カードを無効とする。

【0027】 なお、利用者認証の別の方法として、予め定めたパスワードを計算機カードに暗号化して格納しておき、情報端末装置から入力された文字列が暗号化したものと一致するか否か (又は計算機カードに格納された暗号化されたパスワードを復号したものが情報端末装置から入力されたものと一致するか否か) をチェックする方法、予め定めたパスワードを計算機カードに暗号化して又はそのまま格納しておき、情報端末装置から入力された文字列を、情報端末装置と計算機カードとの間で暗号通信し、入力された文字列が暗号化したもの又はそのままのものとの一致するか否かをチェックし、一致しているか否かによって生成した乱数のパリティを調節し、その乱数を暗号通信する方法、予め定めたパスワードを計算機カードに暗号化して又はそのまま格納しておき、情報端末装置から入力された文字列に情報端末装置で生成した乱数を加えて (あるいは排他的論理和をとって)、

情報端末装置と計算機カードとの間で暗号通信し、計算機カードで送られてきた文字列から予め登録してあるパスワードを引き (あるいは排他的論理和をとって)、得られた値を情報端末装置に返送し、情報端末装置で生成した乱数と返送された値とが一致するか否かでチェックする方法等が適用できる。

【0028】 <利用者選択> 図 7 は利用者選択の工程を示すもので、利用者はメニュー情報から必要な情報を選ぶ。

【0029】 <情報要求> 図 8 は情報を要求するための情報要求の工程を示すものである。

【0030】 利用者は選んだ情報の情報識別子 Req (音楽情報の場合、国際レコーディングコード (ISRC) 等の全世界共通コードや、情報提供者が独自に付与した情報を一意に特定できる番号等) と情報センタ 1 の公開鍵 KPM とその証明書 XPM とを計算機カード 3 へ送信する。

【0031】 計算機カード 3 は認証センタ 4 の公開鍵 KPC で情報センタ 1 の公開鍵 KPM とその証明書 XPM との辻褄が合っていることを確認し、Req に署名して、 $RQS = DK_s(Req)$  なる RQS を得る。これを情報センタ 1 の公開鍵 KPM で暗号化し、 $RU = EK_p(RQS)$  なる RU を情報端末装置 2 に送信する。

【0032】 情報端末装置 2 は RU を受けとると、それに計算機カード 3 の公開鍵 KPU とその証明書 XPU とを付け加えて情報センタ 1 に送信する。

【0033】 情報センタ 1 は送られてきた計算機カード 3 の公開鍵 KPU とその証明書 XPU との辻褄が合っていることを確認し、RU から RQS を  $RQS = DK_p(RU)$  として求め、さらに Req を  $Req = EK_p(RQS)$  として求め、情報を検索する。

【0034】 <情報配送・蓄積・情報センタ認証> 図 9 は情報配送・蓄積・情報センタ認証の工程を示すものである。

【0035】 利用情報 I を暗号化するための鍵 WK を情報センタ 1 が生成し、情報 I を  $C = EWK(I)$  として暗号化し、情報端末装置 2 の情報蓄積部に暗号化されたまま蓄積する。暗号化情報 C が確かに情報センタ 1 から送り出されたものであることを示すためには、これに情報センタ 1 の署名を付ける。なお、ここで、暗号化された情報全体に署名を付けることは効率的でないので、ある一方向性ハッシュアルゴリズム h によって C の量を削減したものの h (C) に対して  $SIM = DK_s(h(C))$  として署名を付ける。

【0036】 情報端末装置 2 は受けとった暗号化情報 C にハッシュアルゴリズムを施し、受けとった SIM と一緒に計算機カード 3 へ送信する。

【0037】 計算機カード 3 はその署名が正しいかどうかを、情報センタ 1 の公開鍵 KPM を用いて  $EK_p(SIM)$  が h (C) と一致するか否かで検証し、要求情報 Re

10

20

30

40

50

q、暗号化された情報端末装置 2 の識別番号 IDS を登録する。

【0038】＜署名・配達証明準備＞図 10 は署名・配達証明準備の工程を示すものである。

【0039】計算機カード 3 は暗号化された情報 C が情報端末装置 2 に蓄積されたことを情報センタ 1 に知らせるため、ハッシュ化された暗号化情報 h (C) に計算機カード 3 の秘密鍵 KSU で署名をし、 $SU = DK_r(h(C))$  なる SU を送信する。

【0040】情報センタ 1 は SU が正しいものであるかどうかを、 $EK_r(SU)$  が h (C) と一致するかどうかで検証する。

【0041】次に、配達証明のために、乱数  $r_i$  ( $i = 0, 1, \dots, t-1$ ) を生成し、 $X_i = IDU^i \bmod n$  により  $X_i$  を求め、 $XX = (X_0 | X_1 | \dots | X_{t-1})$  を情報端末装置 2 を経由して情報センタ 1 へ送信する。但し、t は鍵 WK のビット数で、| は結合を意味する。

【0042】＜鍵配送・配達証明＞図 11 は鍵配送・配達証明の工程を示すものである。

【0043】情報センタ 1 は XX と RQS と WK から  $E = WK \parallel h(XX, RQS)$  を求める。但し、 $\parallel$  はビット毎の排他的論理和を表すものとする。 $E$  を 1 ビットずつに分割し、それを  $e_i$  ( $i = 0, 1, \dots, t-1$ ) とする。

【0044】まず、 $e_i$  を計算機カード 3 に送る。計算機カード 3 では受けとった  $e_i$  に対して、 $Y_0 = S^{e_i} \cdot 0 \bmod n$  を計算し、 $Y_0$  を情報センタ 1 へ送り返す。この時、 $IDU = S \bmod n$  が成り立つように S が定められている。

【0045】 $Y_0$  を受けとった情報センタ 1 は  $Y_0^t \equiv IDU^t \cdot X_0 \bmod n$  が成り立っているかどうかを検証する。成り立っている場合は続けて  $e_i$  を送り、同様に  $Y_1$  を受けとって検証する。これを t 回繰り返す。t 回繰り返された後、情報センタ 1 は RU, SU,  $e_i$ ,  $Y_i$  ( $i = 0, 1, \dots, t-1$ ) を、課金根拠として記録する。

【0046】計算機カード 3 は、送られてきた  $e_i$  を結合して  $E$  を求め、 $WK = E \parallel h(XX, RQS)$  によって、WK を得て、Req, IDS と組になるよう登録する。

【0047】なお、ここでは  $e_i$  の送り方を簡単にするため、1 ビットずつにする方法を述べたが、何ビットかまとめて送る方法もあることはいうまでもない。

【0048】＜情報利用＞図 12 は情報利用の工程を示すものである。

【0049】利用者が情報を利用する時は、計算機カード 3 を情報端末装置 2 に接続して該情報端末装置 2 を操作する。情報端末装置 2 から、乱数 r を含んだ WK 要求メッセージ ReqW が計算機カード 3 へ送信される。計算機カード 3 では ReqW 内の乱数 r と鍵 WK を結合し、そ

れを情報端末装置 2 の公開鍵 KPS で暗号化し、 $V = EK_r(r, (WK, r))$  なる V を情報端末装置 2 に送る。

【0050】情報端末装置 2 では V を KSS を用いて復号した後、r が一致するかどうかをチェックし、鍵 WK をセットし、蓄積された暗号化情報 C を復号し、利用できるようにする。

【0051】なお、KSS を用いて復号する装置から WK で復号する装置までは物理的に機密保持がなされている。その実現方法としては該部分を頑丈な容器に入れ、封印をするか、R.Mori and M.Kawahara 'Superdistribution: The Concept and the Architecture' Trans. IEICE, E-73, No. 7, 1990-7 に記載された方法を適用することが可能である。

【0052】正当な利用者は、正しい計算機カード 3 を持っている限り、情報端末装置 2 に蓄積された情報を何回でも利用することができる。

【0053】＜情報端末装置に情報が蓄積されていない場合の情報利用＞図 13 は情報端末装置に情報が蓄積されていない場合の情報利用の工程を示すものである。

【0054】図 8 と同様に情報要求がなされた後、計算機カード 3 ではその情報要求 Req が登録されているかチェックし、登録されているなら IDS を情報端末装置 1 DS に返送する。情報端末装置 1 DS は別の情報端末装置 1 DS から暗号化情報 C を転送してもらい、図 12 による情報利用で情報を利用する。

【0055】また、転送してもらいつつ情報を利用する方法として、以下の方法がある。情報端末装置 2 は SU を情報センタ 1 へ送り出した後、計算機カード 3 内へ乱数 r を含んだ WK 要求メッセージ ReqW を送信し、計算機カード 3 で ReqW 内の乱数 r と鍵 WK を結合し、それを情報端末装置 2 の公開鍵 KPS で暗号化し、 $V = EK_r(r, (WK, r))$  なる V を情報端末装置 2 に送信する。

【0056】情報端末装置 2 では V を KSS を用いて復号した後、乱数 r が一致するかどうかをチェックし、鍵 WK をセットする。暗号化情報 C を復号し、利用できるようにし、受けとったことを示すために ACK を返送する。この際、復号しながら蓄積するということも可能である。

【0057】なお、前記実施例では ISDN 等の公衆通信回線を利用する場合について示したが、専用線等のコネクションレスの回線にも適用できることはいうまでもない。

【0058】

【発明の効果】以上説明したように本発明によれば、情報が第 3 者に漏れることがないことと、違法コピーが困難であり、さらに配達証明情報により確実に課金を行えることから、情報提供者が安心して利用できるシステムを構成でき、しかも利用者にとって不利になることはなく、利用したい情報が近くの情報端末装置に無くとも、情報センタへアクセスすることにより利用でき、また、

どの情報端末装置からでも利用可能となる等の利点がある。

【0059】なお、本発明は、コンピュータソフトウェアのみならず、全ての暗号化デジタル情報の通信利用による配送の際に適用できることは言うまでもない。

【図面の簡単な説明】

【図1】本発明のデジタル情報保護システムの一実施例を示す図

【図2】情報センタの詳細な構成図

【図3】情報端末装置の詳細な構成図

【図4】計算機カードの詳細な構成図

【図5】計算機カード・情報端末相互認証の工程を示す図

【図6】利用者認証の工程を示す図

【図7】利用者選択の工程を示す図

【図8】情報を要求するための情報要求の工程を示す図

【図9】情報配送・蓄積・情報センタ認証の工程を示す図

【図10】署名・配達証明準備の工程を示す図

【図11】鍵配送・配達証明の工程を示す図

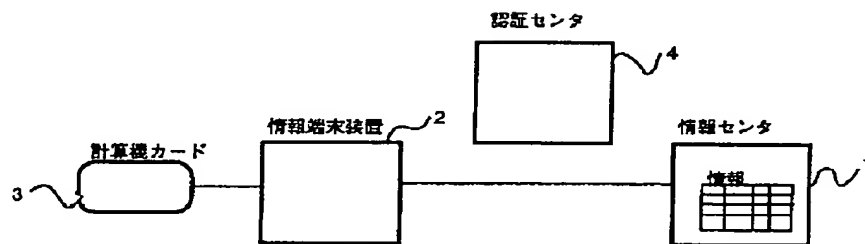
【図12】情報利用の工程を示す図

【図13】情報端末装置に情報が蓄積されていない場合の情報利用の工程を示す図

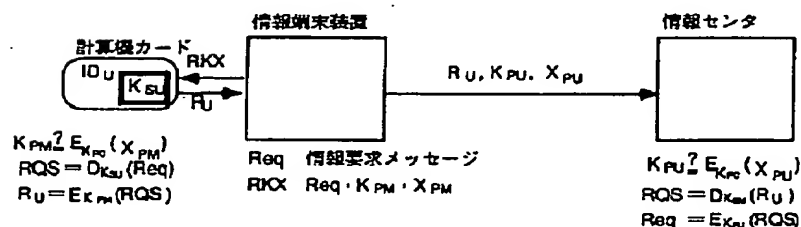
【符号の説明】

1…情報センタ、2…情報端末装置、3…計算機カード、11…情報入力部、12…情報蓄積部、13…情報暗号化部、14…WK生成部、15…公開変換部、16…署名変換部、17…メモリ、18…CPU、19…公開鍵検証部、20…ネットワーク入出力部、21…カード入出力部、22…復号鍵抽出部、23…情報復号部、24…情報出力部、25a…画像表示装置、25b…音声出力装置、26…機密保護手段、27…情報蓄積部、28…ネットワーク入出力部、29…メモリ、30…CPU、31…公開鍵検証装置、32…公開鍵暗号装置、33…通信装置、34…パスワード照合装置、35…復号鍵登録装置、36…メモリ、37…CPU、38…電圧監視装置、39…電池。

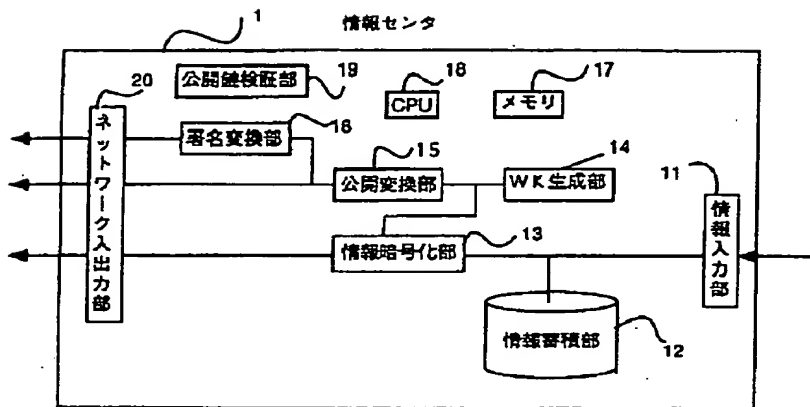
【図1】



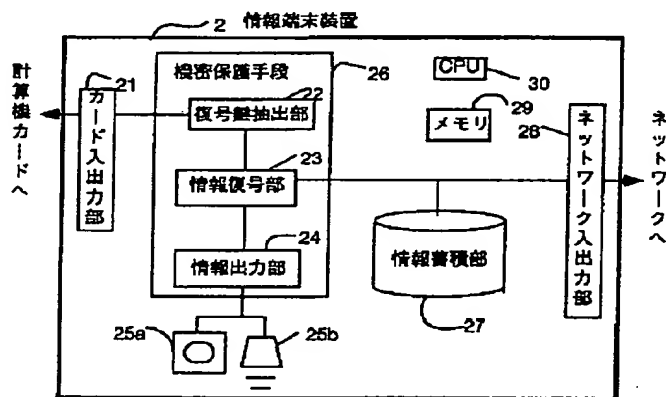
【図8】



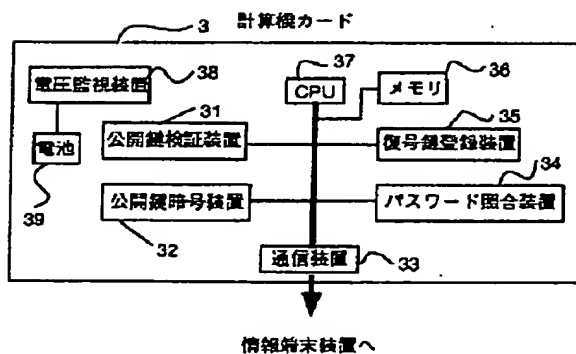
【図 2】



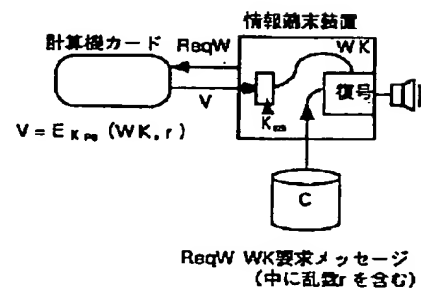
【図 3】



【図 4】



【図 1 2】



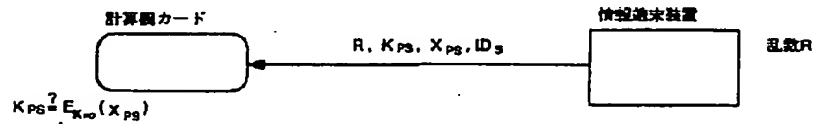


【 図 5 】

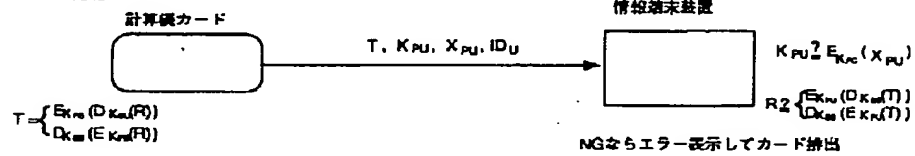
## (1) カード挿入 (受信開始)



## (2) 相互認証開始

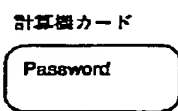


## (3) カード応答

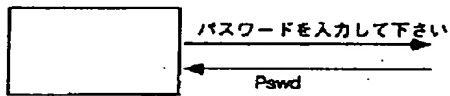


【 図 6 】

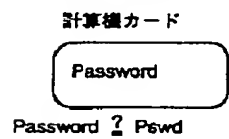
## (1) パスワード入力



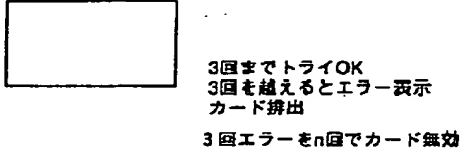
## 情報端末装置



## (2) パスワード照合



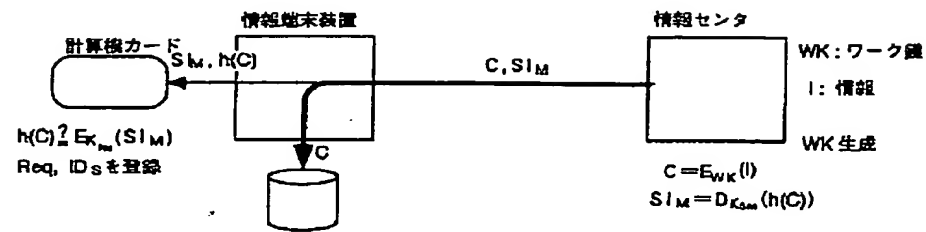
## 情報端末装置



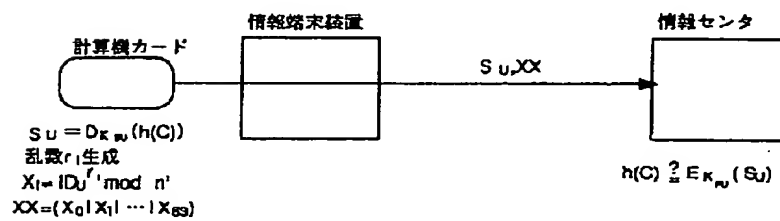
【 図 7 】



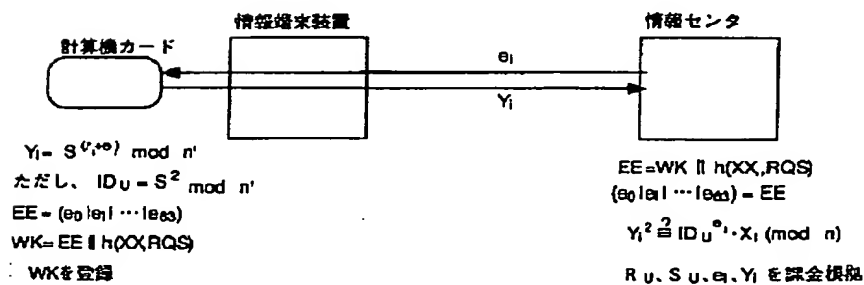
【 図 9 】



【 図 10 】



【 図 11 】



【图 1 3】

